CLAIM OR CLAIMS

[43] What I claim as my invention is:

1. A method for computing the number of points on an elliptic curve over a finite field, in which a Frobenius equation is solved to a given precision by first and second parts, wherein said parts comprise the following steps :

a) Said first part firstly computes a first partial solution of said equation using said first part recursively to reduced precision,

b) Said first part secondly applies a Frobenius operation to said first partial solution,

c) Said first part thirdly computes an error term for said equation,

d) Said first part fourthly computes correction factors for said equation,

e) Said first part fifthly computes a second partial solution using said second part to reduced precision,

f) Said first part sixthly combines said first partial solution and said second partial solution,

g) Said second part firstly computes a first partial solution of said equation using said second part recursively to reduced precision,

h) Said second part secondly applies a Frobenius operation to said first partial solution,

i) Said second part thirdly updates said error term,

j) Said second part fourthly computes a second partial solution using said second part recursively to reduced precision,

k) Said second part fifthly combines said first partial solution and said second partial solution.

2. The method of claim 1 in which said reduced precision is one half of said given precision.

3. The method of claim 1 in which said first and second parts compute the Teichmüller lift of a given finite-field polynomial.

4. The method of claim 1 in which said first and second parts compute the canonical lift of said elliptic curve.

5. The method of claim 1 in which said first and second parts compute the multiplicative representative of a given finite-field element.

6. The method of claim 1 in which said first and second parts compute the trace of a given p-adic number.

7. The method of claim 1 in which said first and second parts compute the norm of a given